Securing the Home Network

October 2012

ON CYBER PATROL
"It's all about the network."
OH, A WITCH AND A VAMPIRE, VERY SCARY!
TRICK OR TREAT
Firewall
HEY LITTLE GUY, WHERE'S YOUR COSTUME? WHAT'S SO SCARY ABOUT PLAYING WITH A TABLET?
Firewall
WHAT IF I TOLD YOU I WAS CONNECTED TO YOUR NETWORK?
Firewall
AUGGHHH!!!
GO BACK TO SLEEP HONEY, OUR NETWORK IS FINE.
KF

Before going to bed, most people ensure they have locked the door and checked the windows to make sure their home is secure; and if they have an alarm system they usually arm it as well. Why do we take such precautions to safeguard our home? We implement these security measures to protect our valuables from theft and harm. Family members, electronic equipment and expensive jewelry are so important that we go to great lengths to protect them. You should ask yourself are you taking the same precautionary measures to protect your home network from intrusion. Many homes have at least one computer and a number of other wireless devices connected to a wireless router. In some locations this wireless router is provided from the local cable company and comes unprotected. This unprotected router is configured from the factory as “open” with no security in place to make it easier to setup. However, it is the responsibility of the homeowner to properly configure the router once it has been delivered.

There are a number of steps a user can take to protect their wireless router against unauthorized access. One of the easiest steps is not to broadcast the service set identification (SSID) for others to pick up. The SSID is the network name and is initially set by the manufacturer. Not broadcasting it will prevent the SSID of your router from being searchable by other wireless devices unless the SSID is programmed into the device. You should also change the default administrator password assigned to your router if it came with one from the factory. Another security measure is to enable MAC address filtering to prevent devices from joining your network that are not listed by MAC address. A less popular but effective step is to assign static IP addresses to each device. It takes more time and knowledge to do this opposed to dynamic hosting but it also keeps hackers from grabbing an accepted IP address from the DHCP pool.

One of the strongest measures you can take is to change the encryption used by your router. The least secure encryption is Wireless Encryption Protocol (WEP) it is also the least recommended because it is easier to crack and much older. To provide your network with the greatest amount of security it is recommended that you use Wireless Protected Access 2 (WPA2) encryption. WPA2 is the successor to Wireless Protect Access (WPA), and is the most recent form of encryption used for home devices. In addition to being newer, it is significantly more difficult to crack than WEP or WPA encryption Also you should take advantage of the measures included with new networking systems. Many routers come with built-in firewalls; but users just have to make sure it is enabled since it usually disabled by default. Personal firewall software should also be run on individual computers as an added security measure. This layered approach will allow the router to protect your network from outside intrusion, while the software firewall on each computer will protect the individual computers from intrusion within the network should any system be compromised. Implementing all of the precautions listed above is not guaranteed to stop a skilled and determined hacker, but it will greatly reduce your chances of becoming a victim.

In the modern digital age, the importance of securing your home network cannot be overlooked. Many of us perform online banking, online shopping, send online payments, telework from home, or store our tax return and other personal information on our computers. All of which is information a skilled computer hacker would love to easily access through an unsecured wireless connection. Additionally, if you leave your router "open" because you aren't concerned about someone using your internet connection from outside your house, remember that if they are accessing websites with illegal content, illegally sharing or downloading digital media files such as music or movies, or if they are using your connection to illegally hack other computer systems, it is you the authorities will come for. Since your router is in your house, and is associated with your address, it is your responsibility to ensure that it is not being used for nefarious purposes. Otherwise, your neighbor's internet activity could make trouble for you.

Remember, it's just as equally important to secure your home network as it is to lock your front door. So be sure to shut your windows, lock your doors, and secure your router to keep the uninvited from entering your home.